Confidentiality of health data in contact tracing systems during the Covid-19 pandemic in France

Antoine Berar, Renaud Bouvet

CONFIDENTIALITY OF HEALTH DATA IN CONTACT TRACING SYSTEMS DURING THE COVID-19 PANDEMIC IN FRANCE

Article category: Article

KEY POINTS

- The goal of contact tracing is to identify individuals who have come into contact with people diagnosed with a communicable disease. The manual and digital contact tracing systems implemented in France to mitigate the spread of the virus responsible for Covid-19 had to comply with the EU General Data Protection Regulation and national legislation.
- They provided a certain number of guarantees in relation to data protection. Notably, infected people were not obliged to disclose the identity of their contacts to contact tracers who requested this information during manual contact tracing. With regard to digital contact tracing, individuals were free to choose whether they downloaded and installed the application on their smartphones and the data processed by the application were pseudonymised, i.e. did not contain any names. The duration of these systems was originally limited, but the end date has been repeatedly pushed back.
- The systems also raised issues about the confidentiality of processed data. Data obtained by contact tracers during their interviews with infected subjects were entered into an information system, called Contact Covid, which was astonishing in terms of the extent of data collected, both on infected people and their contacts, and the number of people who can access these data. There is also a risk that infected people are identified by users of the digital contact tracing application and risks arising from the centralised nature of the system, including that of contacts being identified by the authorities.

KEYWORDS

Confidentiality; Contact tracing; Communicable disease; Covid-19; Digital tools; Health data;

INTRODUCTION

SARS-CoV-2 emerged in late 2019 and had become, within a few months, the focus of global attention due to its high transmissibility and its ability to cause acute respiratory failure, especially in the elderly and in people with comorbidities.[1] Most governments, faced with a pandemic of a magnitude unprecedented in the 21st century,[2] adopted emergency measures to reduce or stop the spread of the virus.

Contact tracing is a well-established practice that consists of identifying people who have come into contact with infected people. During the Covid-19 pandemic, contact tracing was carried out using new methods. Manual contact tracing (MCT), in which the key stage consists of interviewing infected subjects in order to identify their contacts,[3] has involved the collection and recording of data in electronic databases.[4] In parallel, digital contact tracing (DCT), in which notification of infection risk uses a smartphone application, was implemented for the first time in a pandemic, although the principle had already been described.[5]

France deployed an MCT system and a DCT application. Both systems process personal data. In MCT, the data are intended to form part of a filing system, while in DCT, their processing involves automated means. Therefore, France, as a member state of the European Union (EU), was bound by the provisions of the EU General Data Protection Regulation (GDPR), which regulates the processing

[1] Rachel E Jordan, Peymane Adab and KK Cheng, 'Covid-19: Risk Factors for Severe Disease and Death' (2020) 368 BMJ (Clinical research ed.) m1198.

[2] David M. Morens and others, 'Pandemic COVID-19 Joins History's Pandemic Legion' (2020) 11 mBio e00812.

[3] ibid.

[4] 'Digital Tools for COVID-19 Contact Tracing' <https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1> accessed 9 January 2022.

[5] Seungyeon Jeong, Seungho Kuk and Hyogon Kim, 'A Smartphone Magnetometer-Based Diagnostic Test for Automatic Contact Tracing in Infectious Disease Epidemics' (2019) 7 IEEE access: practical innovations, open solutions 20734.

of personal data.[6] The GDPR notably prohibits the processing of health data with derogations permitted in a few, enumerated situations.[7] Consequently, in deploying its MCT system and creating its DCT application, both of which process health data, the French government invoked one of the derogations enumerated by the article 9 of GDPR. Furthermore, France was also bound by its own legislation, which includes the right to respect for private life, of both constitutional[8] and legal[9] validity and the professional duty of confidentiality incumbent on health professionals that underpins the patient's right to secrecy, both of which have legal validity.[10] A legal derogation to the right to secrecy was therefore necessary for MCT as it requires that health professionals share data about infected people; a purpose of constitutional validity was also invoked to justify the data sharing.

It is important however to examine exactly how much confidentiality the authorities accorded to health data in the combat against the pandemic. Perceived confidentiality is a major determinant of the population's level of trust in these systems and the trust itself is a prerequisite for their effectiveness. In short, an effective MCT system is impossible without the cooperation of people with Covid-19, who are requested to share their recollection of their recent activities and interactions. Similarly, DCT requires a threshold level of cooperation by the population in order to have a chance of reducing the circulation of the Covid-19 virus.[11]

---

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[7] Art. 9 of the GDPR.

[8] Const. Council, 23 Jul. 1999, decision no. 99-416.

[9] Art. 9 of the Civil Code.

[10] Art. L. 1110-4 of the Public Health Code (Code de la santé publique, CSP).

[11] 'Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us out of Lockdown' <https://www.research.ox.ac.uk/article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown> accessed 20 January 2022.

The scope of our analysis is the health data processed by these contact tracing systems. In line with the spirit of the French medical code of ethics, according to which the duty of confidentiality is not limited to health data alone but also covers "*everything that comes to the knowledge of the physician in the exercise of his/her profession*",[12] our analysis will also look at non-medical data collected by healthcare system stakeholders for the purposes of MCT. Then, after positioning contact tracing in the toolbox of measures against Covid-19, we will examine the confidentiality of data first within the context of MCT then that of DCT.

[12] Art. R. 4127-4 of the CSP.

I. THE SEARCH FOR SOLUTIONS FOR TRACING COVID-19 INFECTION CHAINS

1. *A Strategy Supporting the Path ouf of Lockdown*

The first cases of Covid-19 on French soil were officially detected at the end of January 2020.[13] Less than two months later, the first wave of the Covid-19 pandemic led to the imposition of a period of lockdown, from 17 March 2020[14] to 11 May 2020.[15]

A wide range of measures still remained necessary to limit viral transmission between individuals. The French government, like so many others worldwide, therefore decided to deploy systems for the early identification and quarantine of subjects liable to transmit Covid-19. This goal translated into the implementation from 13 May 2020 of MCT, which was primarily conducted by Assurance Maladie (the French health insurance system) on the basis of data provided by index patients (i.e. the individuals diagnosed with Covid-19),[16] and the launch on 2 June 2020 of a smartphone application, which would be able to reconstitute chains of transmission involving densely packed places and unknown people, thereby remedying one of the weaknesses of MCT. These two methods had distinct characteristics.

2. *MCT by Healthcare System Stakeholders*

[13] Sibylle Bernard Stoecklin and others, 'First Cases of Coronavirus Disease 2019 (COVID-19) in France: Surveillance, Investigations and Control Measures, January 2020' (2020) 25 Eurosurveillance 2000094.

[14] Order of 14 March 2020 concerning various measures for the combat against the spread of the Covid-19 virus 16; Decree no. 2020-260 of 16 March 2020 concerning the regulation of movements in the context of the combat against the spread of the Covid-19 virus.

[15] Decree no. 2020-548 of 11 May 2020 prescribing the general measures necessary to combat the Covid-19 epidemic in the context of the state of health emergency.

[16] Art. 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

MCT aims to reconstitute the chains of potential transmission of a disease so that individuals coming into high-risk contact with an infected person are informed that they are at risk of developing the disease themselves. As part of the system implemented in France from May 2020, individuals infected with Covid-19 are interviewed and asked to identify people they came into high-risk contact with, solely on the basis of their recollection of recent interactions. The people considered to be contacts at high risk of being infected are then contacted and urged to undergo a Covid-19 screening test and to quarantine. Data from these interviews are collected in an information system called Contact Covid.

The best results of MCT are achieved when all individuals infected with Covid-19 are identified. For this reason, another information system, SI-DEP (*système d'information de dépistage populationnel* or population screening information system) was developed to centralise the results of Covid-19 diagnostic tests.[17] With SI-DEP in place, it becomes possible to rapidly inform the different stakeholders involved in MCT.

This method, in which all the high-risk contacts identified by the infected person are individually contacted, requires a huge amount of time and human resources. Furthermore MCT has inherent weaknesses: patients cannot identify people who were in close proximity to them but are strangers; the fallible nature of human memory; and the potential reticence in providing information about one's private life.[18] These are the reasons why DCT, in the form of a smartphone application, was deployed to supplement MCT.

3. *DCT Using the StopCovid Application*

After the first lockdown ended, the French government proposed a DCT method. DCT differs from MCT in many ways: it is based on devices, smartphones, rather than on recollection by patients. No

[17] Law no. 2020-1379 of 14 November 2020 authorising the extension of the state of health emergency and concerning various measures for managing the health crisis.

[18] Philippe Bas and others, 'Covid-19 : Deuxième Rapport d'étape Sur La Mise En Œuvre de l'état d'urgence Sanitaire' (2020) 608.

healthcare system stakeholders are directly involved. Lastly, it is available to the entire population, consistent with the logical assumption that every person is a potential vector of the virus.

Several methods of DCT were designed around the world.[19] With regard to their technical characteristics, the main differentiator was whether they use Bluetooth technology, whether they locate individuals using GPS signals or whether, more rarely, they use WiFi or QR codes. The DCT method implemented in France was a voluntary smartphone application using Bluetooth technology. The application determines which individuals have recently been in close proximity to another user who self-declared as having Covid-19; it attempts to raise awareness among these high-risk contacts about disease symptoms and protective measures, and to guide them to competent health stakeholders.

Both MCT and DCT raise questions about the confidentiality of the data they process.

[19] Nasro Min-Allah and others, 'A Survey of COVID-19 Contact-Tracing Apps' (2021) 137 Computers in Biology and Medicine 104787.

II. MCT: A WIDE RANGE OF HEALTHCARE SYSTEM STAKEHOLDERS WITH ACCESS TO A LARGE AMOUNT OF PERSONAL PATIENT DATA

1. *Development of the SI-DEP and Contact Covid Information Systems: a Doubly Criticised Choice*

The implementation of MCT via the SI-DEP and Contact Covid systems was far from being the sole domain of doctors; several stakeholders had access to data about infected people and their contacts. This state of affairs was criticised on two counts: first, it represented a breach of the duty of confidentiality to which all health professionals are bound; second, Covid-19 could simply have been added to the existing list of notifiable diseases.

First, the fact that healthcare system stakeholders who are not the professionals to whom personal data are entrusted have access to the data represents a derogation to the principle of the *"right to the respect for one's private life and the confidentiality of data about one's private life"*[20] laid down in French legislation for all people receiving care from a healthcare professional or a healthcare establishment. This situation was criticised on the grounds that it could jeopardise the trust that every patient should have in their doctor, and also the trust that society as a whole should have in the medical profession.[21] The combat against human immunodeficiency virus (HIV) in the past was held up as a good example of a public health policy that refrained from removing the professional duty of confidentiality. Nevertheless, HIV and Covid-19 are not completely comparable: Covid-19 transmission does not require intimate contact and symptoms develop quickly in infected people. For these reasons, certain doctors advocated for the derogation to the professional duty of confidentiality as part of the battle against Covid-19.[22]

[20] Art. L. 1110-4 of the CSP.

[21] Brigitte Feuillet-Le Mintier, 'Les fondements du secret médical' (2000) 13 Revue Juridique de l'Ouest 1; Patrick Verspieren, 'Le secret médical et ses fondements' (2007) Vol. 55 Laennec 6.

[22] Philippe Biclet, 'Non, Le COVID Ne Mérite Pas Les Justes Combats de l'époque Du Sida Pour Le Respect Du Secret Médical' (2021) 2021 Médecine & Droit 3.

Second, the criticism levelled at MCT was less for the derogation to the professional duty of confidentiality than for the new tools developed for this purpose, the SI-DEP and Contact Covid systems. In itself, there is nothing new about allowing healthcare system stakeholders to share data about the health of a given person for a greater good. The law notably provides for the transfer of data about individuals to health authorities as part of the combat against a certain number of diseases of public health significance. All healthcare professionals concerned, biologists as well as clinicians, are legally obliged to transfer such data and the transfer does not require the patient's consent. Thirty-six diseases, so-called 'notifiable diseases', are covered by this obligation, including thirty-one infectious diseases. Despite common characteristics with some of them, the French legislator decided against adding Covid-19 to the existing list of notifiable diseases, choosing instead to create the new SI-DEP and Contact Covid systems. This decision has been questioned, especially because the criteria normally used by the High Council for Public Health (*Haut conseil de la santé publique,* HCSP) seem to support the inclusion of Covid-19 in the list of notifiable diseases.[23] Moreover the HCSP referred to these criteria in a recent decision.[24] In fact, it is likely that the legislator's decisions were guided by the magnitude of the procedures necessary in the context of such a pandemic. The Minister of Health explained that "*the notifiable diseases system is more suited to slow progressing diseases*".[25] The HCSP considered, in 2016, that a notifiable disease *"should not be too frequent as this guarantees a good level of notification and allows regional health agencies to respond rapidly*".[26]

[23] Bruno Py, 'De la surveillance des maladies à la surveillance des malades' (*Dalloz Actualité*, 27 May 2020) <https://www.dalloz-actualite.fr/node/de-surveillance-des-maladies-surveillance-des-malades#.YO_oHOgzbIU> accessed 12 January 2022.

[24] HCSP, 'Avis relatif à l'inscription de l'encéphalite à tiques sur la liste des maladies à déclaration obligatoire' (2020).

[25] Vincent Bordenave, 'Est-il obligatoire de déclarer que l'on a le coronavirus ?' *Le Figaro (website)* (12 May 2020).

[26] HCSP, 'Infection par le virus Zika : inscription sur la liste des maladies à déclaration obligatoire' (2016).

This decision had substantial consequences. With regard to formal aspects, it required a new law, whereas adding a disease to the existing list of notifiable diseases would only have required a decree.[27] In practical terms, the law of 11 May 2020 behind the development of SI-DEP and Contact Covid, and its implementing decree of 12 May 2020 expanded, in comparison to the notifiable diseases system, the nature of data that were shared and the number of people with access to them.

2. *Law no. 2020-546 of 11 May 2020*

Since the law of 4 March 2002, article L. 1110-4 of the Public Health Code has guaranteed the *"right to the respect for one's private life and the confidentiality of data about one's private life"* for all patients.[28] It also provides for a certain number of derogations to this principle, including the possibility of sharing these data with professionals who are not part of the same care team subject to the patient's consent. The law of 11 May 2020 stipulated that SI-DEP and Contact Covid are created "*by derogation to article L. 1110-4 of the public health code*",[29] thereby creating a new derogation to the right to confidentiality, which in this instance dispenses with the need for consent of the people concerned. In other words, the processing of personal data by SI-DEP and Contact-Covid is not based on the consent of subjects: this legal basis, provided by the GDPR,[30] would have prevented the contact tracing of non-consenting subjects, which was not acceptable from the authorities' point of view. Besides, in the context of a health crisis, the freedom to consent could have been considered weakened, especially because consent must be explicit when it concerns health data. Finally, independently of the pandemic context, the GDPR considers that consent may not be free when given to a public body, given the body's potential powers.

[27] Art. L. 3113-1 of the CSP.

[28] Law no. 2002-303 of 4 March 2002 concerning the rights of patients and the quality of the health system.

[29] Art. 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

[30] Art. 6 of the GPDR.

In fact, legal basis of SI-DEP and Contact-Covid are the "*performance of a task carried out in the public interest*"[31] and "*reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health*".[32] In this case, Union or Member State law must authorize the data processing. The law of May 11, 2020 was therefore necessary to comply with the requirements of the GDPR.

Domestically, the law of 11 May 2020 underwent an a priori constitutionality review by the Constitutional Council to ensure that it was not breaching any rules of constitutional validity. In this particular case, the constitutionality of the provisions creating SI-DEP and Contact Covid were essentially evaluated from the perspective of respect for private life, a right that had been granted constitutional validity by past case law of the Constitutional Council.[33]

In its decision of 11 May 2020,[34] the Constitutional Council considered that the provisions of the law breached the right to the respect for private life. It also considered however that the measures taken by the law seek to safeguard health, a purpose of constitutional validity[35] and one that is also in the general public interest and hence the breach was justified. There followed a test of proportionality, by which the Constitutional Council assesses whether the legislator has struck the right balance between the right to respect for private life and the safeguarding of health. The judges issued a positive opinion for some aspects of the law – e.g., the limitation of the use of SI-DEP and Contact Covid to four, restrictively listed purposes. With regard to the data being processed, the Constitutional Council considered that the legislator had limited them to "*only the data that are strictly necessary to achieve*

[31] ibid.

[32] Art. 9 of the GPDR.

[33] Vincent Mazeaud, 'La Constitutionnalisation Du Droit Au Respect de La Vie Privée' [2015] Les Nouveaux Cahiers du Conseil constitutionnel 7.

[34] Const. Council, 11 May 2020, decision no. 2020-800.

[35] Paragraph 11 of the preamble to the Constitution of 27 October 1946.

the first three purposes".[36] However, in relation to the 'epidemiological surveillance and research' purpose, which does not require personal identifier data, the Constitutional Council considered that the telephone number and email address should be deleted out of respect for private life, such as first and last names. In relation to the people who have a right to access the data without the consent of the people concerned, the Constitutional Council stated that the list was particularly broad but recognised that this was a necessity due to the "*quantity of procedures to be undertaken to organise the collection of data required to combat the development of the epidemic*".[37] However, it censured as ignoring the right to respect for private life the fact that this list included entities providing social care to the people concerned, insofar as they do not directly participate in the combat against the epidemic. Although partially censured by the Constitutional Council in its decision of 11 May 2020, the list of people with access to the data shared via SI-DEP and Contact Covid remained considerable. The list included not only the Minister of Health, the National Public Health Agency, Assurance Maladie entities and regional health agencies (*Agences régionales de santé,* ARSs), but also

> *the armed forces health services, Territorial Professional Health Communities, health, social and medicosocial establishments, community health teams (...), health centres; occupational health services (...) and doctors attending to the people concerned, pharmacists, support systems for the coordination of complex health pathways (...), the specific regional systems mentioned in article L. 6327-6 of the same code, the existing support systems tasked with incorporating them (...) and laboratories and services authorised to carry out relevant laboratory examinations and medical imaging studies on people concerned*.[38]

Furthermore, services performing necessary interventions are permitted under the law to use the services of third-party entities for data processing: in practical terms, the law allows contact tracing interviews to be outsourced. The sheer quantity of stakeholders is in stark contrast to the limited

[36] Const. Council, 11 May 2020, decision no. 2020-800.

[37] ibid.

[38] Art. 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

number of people involved in reporting notifiable diseases: specifically data are transferred to the ARS doctor, then they *"may be transmitted to other professionals whose intervention is essential*".[39] Here, there is not an a priori transfer to a group of people, but a targeted transfer determined by necessity.

The Constitutional Council notes that the authorised entities only have access to the data they need for their intervention, and that their employees, bound by a professional duty of confidentiality, are not authorised to communicate the identity of an infected person to their contacts, unless express consent is given. The law of 11 May 2020 considered it useful to highlight that disclosure of data contained in SI-DEP and Contact Covid could give rise to criminal proceedings. However, multiplying the possibilities of access to personal data increases the risk of a confidentiality breach is commensurate with this number. As the maxim goes "*The more people who know the secret, the less of a secret it becomes*".[40]

Despite its reserves, the Constitutional Council concluded that the provisions for the creation of SI-DEP and Contact Covid "*do not breach the right to respect for private life*" or any other constitutional requirements.[41] This distinctive strategy employed by the Constitutional Council, whereby it does not declare a law as unconstitutional but indicates how to apply it, has been criticised on the grounds that it allows it to impose its own version of the law to the detriment of the legislator's original intent.[42] Conversely, a censure would have obliged Parliament to debate the text again and would have prevented the role of the Constitutional Council from morphing into one of a *"corrective or even positive legislator*".[43]

---

[39] Art. R. 3113-4 of the CSP.

[40] Bruno Py, 'Cent Ans de Secret Professionnel' [2021] Revue droit & santé 230.

[41] ibid.

[42] Damien Fallon, 'Prolongation de l'état d'urgence sanitaire : le Conseil constitutionnel reste confiné dans sa zone de confort' (*JP blog*, 20 May 2020) <https://blog.juspoliticum.com/2020/05/20/prolongation-de-letat-durgence-sanitaire-le-conseil-constitutionnel-reste-confine-dans-sa-zone-de-confort-par-damien-fallon/> accessed 12 January 2022.

[43] ibid.

3. *The Decree of 12 May 2020*

The decree of 12 May 2020, implementing the law of 11 May 2020, officially created the Contact Covid and SI-DEP systems.[44] It had also been charged with specifying which services and people could access the data and also the categories of data they could access and the modalities by which the people concerned could exercise their rights. As provided for in the law of 11 May 2020, the publication of the decree was preceded by examination of the text by the French data protection agency (*Commission nationale de l'informatique et des libertés,* CNIL), an independent administrative authority. In its opinion of 8 May 2020, CNIL basically analysed whether the text complied with GDPR requirements.[45] This opinion makes clear the CNIL's role in protecting personal data but also reveals the limits of this protection.

Generally speaking, CNIL points out that the purposes for which SI-DEP and Contact Covid were developed seem "*quantified, explicit and legitimate"*,[46] in compliance with article 5 of the GDPR. Although it recognises that the information systems are an appropriate response to the pandemic, it insists on the need for them be periodically reevaluated taking into account the evolution of the epidemic and of scientific knowledge. With this requirement, the CNIL demonstrates its dynamic vision of the principle of proportionality: it suggests that a tool considered proportionate at the beginning of a pandemic may no longer be so if the pandemic fades or if scientific knowledge demonstrates its lack of usefulness.

CNIL noted some of the specific guarantees contained in the draft decree, notably emphasizing the voluntary nature of participation in contact tracing interviews – although the processing of data does

[44] Decree no. 2020-551 of 12 May 2020 concerning the information systems mentioned in article 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

[45] Deliberation no. 2020-051 of 8 May 2020 delivering an opinion on a draft decree concerning the information systems mentioned in article 6 of the bill extending the state of health emergency.

[46] ibid.

not rely on consent as a legal basis. That is, infected people are under no obligation to reveal the identity of their contacts, and contacts are not obliged to cooperate with the tracers. Similarly, doctors are not obliged to declare their patients in Contact Covid – although laboratories are obliged to enter the data of all people tested into SI-DEP.

CNIL also noted that the health data processed were limited, i.e. that these data needed to be processed to achieve the stated purposes. Nevertheless, we hasten to point out that even though the extent of data processed by SI-DEP and Contact Covid corresponds to the predefined purposes, it is still considerable. Admittedly, the data collected for entry into SI-DEP are, logically in view of its purpose, relatively limited: identity and contact details of the person tested, position (e.g. health professional or inpatient), date of onset of symptoms (where applicable), identity and contact details of doctors, useful data about the sample (place, date, etc.) and test data including of course the result. Conversely, the data used by Contact Covid, intended to be used to arrange contact tracing interviews, are much more wide-ranging. In addition to the data on the health professional or establishment entering the data, there are also data about the index patient (the person with Covid-19), each of their contacts (defined as people who had come into close proximity with the index patient in the 14 days before the diagnosis, during which time the patient could have been contagious) and even, after the decree of 20 January 2021, about co-exposed people, i.e. individuals who were at the same place, gathering or event as an index patient in the 14 days before they were diagnosed with Covid-19 and where full compliance with protective measures was not possible.[47] Some of these data are also identity data and contact details of people. Although these are general data, it is nevertheless remarkable that certain people, those designated as contacts or co-exposed people, are included in Contact Covid when they may not even be ill – admittedly they can, a posteriori, exercise their right to object. Incidentally, the draft decree denied this right so as not to weaken the identification of contamination chains, but on the

[47] Decree no. 2021-48 of 20 January 2021 modifying chapter I of decree no. 2020-551 of 12 May 2020 concerning the information systems mentioned in article 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

request of CNIL, the decree of 12 May 2020 reinstated this right for contacts; the right to object remains virtually impossible for index patients however.

In addition to these general data, there are also personal health data that are strictly limited "*to the person's viral or serological status*" as regards Covid-19 "*and supporting evidence from the clinical diagnosis and medical imaging*".[48] Alongside these are several other items of data concerning people's private, even intimate, life; these notably include, for index patients and their contacts (and co-exposed people from January 2021),[49] regions or countries visited, presence in specific categories of establishment (health or medicosocial establishments, but also schools, nurseries, prisons and tourist accommodation)[50] and participation in the last 14 days in gatherings of more than ten people. For the last item, the date and location of the gathering are collected, and – following publication of the decree of 14 November 2020 – its purpose ("*sporting event; cultural event; family gathering, celebratory event; gathering for professional reasons; other type of gathering"*).[51] The date of the last contact between the index patient and every contact is also recorded.

The fact that the data collected about contacts are the same as those collected about people with a confirmed infection raises questions about compliance with the purposes of Contact Covid. As far as contacts are concerned, the purposes, as mentioned in article 1 of the decree, are to identify and guide them towards quarantine measures, to follow them medically and to support them during this period.

[48] Art. 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

[49] Decree no. 2021-48 of 20 January 2021 modifying chapter I of decree no. 2020-551 of 12 May 2020 concerning the information systems mentioned in article 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

[50] Decree no. 2020-1018 of 7 August 2020 applying article 3 of law no. 2020-856 of 9 July 2020 organising the exit from the state of health emergency and modifying decree no. 2020-551 of 12 May 2020 concerning the information systems mentioned in article 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

[51] Decree no. 2020-1385 of 14 November 2020 modifying decree no. 2020-551 of 12 May 2020 concerning the information systems mentioned in article 11 of law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions.

Data such as the profession of contacts, the places they have visited, their recent participation in gatherings, their presence at certain sites, hardly seem relevant. The collection of these data on contacts also cannot be justified on the grounds that they can be used to identify their contacts, given that the first-degree contact may not be ill, in which case the second-degree contacts are not contacts. The health minister explicitly stated that "*Contacts of contacts are not contacts*".[52] In short, all these data, in a good number of cases, are destined to remain unused. This seems non-compliant with the minimisation principle imposed by article 5 of the GDPR.

It is easy to justify the collection of all kinds of data on the basis of apparently legitimate purposes.[53] Notably, the 'scientific research' purpose could be used to justify the collection of a wide range of data given that research is based on unproven hypotheses and protocols with goals and needs not yet defined. However, in our opinion it would have been preferable to further limit the amount of data collected because the more data are collected, the greater the consequences of a breach and the greater the possibility that someone succumbs to the temptation to use the data for a purpose other than the stated ones. Moreover, the fear of a confidentiality breach likely increases the likelihood that the people concerned will hide the most sensitive data when mentioning their recent activities. Here, once again, Contact Covid is different to the report submitted with notifiable diseases in that an a priori large amount of data are transferred; in contrast, for notifiable diseases, additional data beyond the diagnosis are only submitted on request of the ARS doctor when such data are deemed "*necessary to implement investigation and intervention measures*".[54] The latter seems more respectful of the principle of proportionality.

CNIL had to formulate several requests to render the decree compatible with certain GDPR requirements. Notably, it called for the rights of access to information (of the index patient and contacts) and to rectification to be guaranteed. Finally, CNIL considered that the government's

[52] Richard Duclos, '"Les cas contacts de cas contacts ne sont pas des cas contacts" : qu'a voulu dire Olivier Véran ?' *LCI (website)* (17 September 2020).

[53] Wacksman (n 10).

[54] Art. R. 3113-4 of the CSP.

proposed text was generally compatible with the GDPR, and that the decree published in the Official Journal on 12 May 2020[55] took into account the requests it had formulated.

The constitutionality test by the Constitutional Council and CNIL's opinion influenced the content of the enacted texts. The input of these two bodies reinforced confidentiality with regard to certain aspects of the systems in question. Nevertheless, the extent of data sharing remained quite vast, in relation to both what was shared and with whom. So it was necessary to place a time limit on the use of these information systems and to establish a storage period for the data.

4. *Time Limits for the Information Systems and Data Storage*

The law of 11 May 2020 authorises the use of the SI-DEP and Contact Covid systems only for the period strictly necessary to combat the spread of the Covid-19 epidemic and for a maximum period of six months from the end of the state of health emergency. By explicitly linking the duration of the information systems to the end of the state of health emergency, even if only a maximum time limit, the legislator provided a guarantee that the information systems would not continue indefinitely after the state of health emergency had ended. As such, the rules applicable to the imposition of a state of health emergency and its extension should also be seen as guarantees for contact tracing too. It is worth nothing that a state of health emergency can only be declared, by decree, "*when a health catastrophe endangers, by its nature and its seriousness, the health of the population*".[56] Furthermore, any "*extension to the state of health emergency longer than one month can only be authorised by a law*", which would specify its duration.[57] The state of health emergency was imposed twice, first from

[55] 'Déconfinement : L'avis de La CNIL Sur Le Projet de Décret Encadrant Les Systèmes d'information Mis En Œuvre Pour Le Suivi Des Malades Du COVID-19 | CNIL' (13 May 2020) <https://www.cnil.fr/fr/deconfinement-lavis-de-la-cnil-sur-le-projet-de-decret-encadrant-les-systemes-dinformation-mis-en> accessed 12 January 2022.

[56] Art. L. 3131-12 et seq. of the CSP.

[57] ibid.

24 March 2020 to 10 July 2020 then from 17 October 2020 to 1 June 2021, the second followed by a transitional regimen for exiting the health crisis.[58]

Yet, the information systems have been maintained. The law of 11 May 2020 granted the legislative body the exclusive right to extend the duration of the information systems beyond the duration initially planned. The legislator exercised this right in four successive laws,[59] which defined new end dates for the use of SI-DEP and Contact Covid (1 April 2021, then 31 December 2021, 31 July 2022 and currently 31 January 2023) thereby breaking the link with the state of health emergency and conferring autonomy to the information systems. The regrettable uncoupling of the expiry date of SI-DEP and Contact Covid from the state of health emergency invariably increased fears, expressed by certain people, that tools originally presented as temporary would become permanent.[60] Moreover, CNIL expressed regret in its opinion of September 2020 that the government, obliged by the law of 11 May 2020 to send a detailed report on SI-DEP and Contact Covid to Parliament every 3 months, did not provide sufficient justification for the decision to maintain these tools when the circulation of the virus had diminished.[61] It remains to be seen how Covid-19 will be declared to health authorities in the future but at the moment there does not seem to be much momentum for adding Covid-19 to the list of notifiable diseases.

---

[58] Law no. 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions; Decree no. 2020-1257 of 14 October 2020 declaring the state of health emergency; Law no. 2021-160 of 15 February 2021 extending the state of health emergency.

[59] Law no. 2020-1379 of 14 November 2020 authorising the extension of the state of health emergency and concerning various measures for managing the health crisis; Law no. 2021-160 of 15 February 2021 extending the state of health emergency; Law no. 2021-1465 of 10 November 2021 concerning various health vigilance provisions; Law no. 2022-1089 of 30 July 2022 ending the exceptional regimes created to fight the epidemic linked to Covid-19.

[60] Py (n 62); Caroline Zorn, 'État d'urgence pour les données de santé (II) : sidep et contact covid' (*Dalloz Actualité*, 26 May 2020) <https://www.dalloz-actualite.fr/flash/etat-d-urgence-pour-donnees-de-sante-ii-sidep-et-contact-covid#.YPAMWegzbIU> accessed 12 January 2022.

[61] Deliberation no. 2020-087 of 10 September 2020 delivering a public opinion on the implementation conditions of the information systems developed for combating the spread of the COVID-19 epidemic (May to August 2020).

As regards the duration of data storage, the law of 11 May 2020 stipulated a maximum period of 3 months from the date of their collection, a provision accepted by the Constitutional Council in the constitutionality test of 11 May 2020.[62] However the law of 9 July 2020 established that the storage period of personal data for the purposes of epidemiological surveillance and research[63] could be extended by decree; the Constitutional Council did not object to these provisions during a constitutionality test.[64] Although the data transferred to the entities carrying out these purposes would be pseudonymised (stripped of all data that directly identified people), the French Medical Council severely criticised the change. It denounced the change as a turnaround contrary to the engagements that had been made, stressing its role as "*the guarantor of medical privacy*" and stating that its support for the development of Contact Covid and SI-DEP had been partly based on the data storage period initially guaranteed.[65]

[62] Const. Council, 11 May 2020, decision no. 2020-800.

[63] Law no. 2020-856 of 9 July 2020 organising the exit from the state of health emergency.

[64] Const. Council, 9 July 2020, decision no. 2020-803.

[65] Conseil National de l'Ordre des Médecins, 'Fichiers SIDEP et AmeliPro' (15 June 2020) <https://www.conseil-national.medecin.fr/publications/communiques-presse/fichiers-sidep-amelipro> accessed 16 January 2022.

III. DCT: DESIGNED WITH PRIVACY IN MIND BUT NOT WITHOUT FLAWS

1. *The Quest of Privacy by Design*

The free smartphone application StopCovid was officially adopted by the decree of 29 May 2020[66] and made available on 2 June 2020 shortly after the end of the first lockdown. Like MCT, StopCovid set out to bring the Covid-19 pandemic under control while minimising restrictions to individual freedoms. It was updated and renamed TousAntiCovid on 22 October 2020.

Several guarantees related to the application were mentioned as early as the announcement of its launch by the Minister of Health and the Secretary of State for Digital Affairs, on 8 April 2020: participation would be voluntary; individuals would not be geolocalised or identified; the application would be time-limited as it was not intended to exist longer than the health crisis.[67] These guarantees are part of the privacy by design approach encouraged by article 25 of the GDPR whereby the development of the application is not only based on purely technical considerations but also seeks, from the outset, to comply with the standard imposed by the texts.[68]

An opinion was first sought from CNIL while the application was still under development.[69] CNIL confirmed that StopCovid processed personal data: the data were deemed personal because they maintained a link with individuals via the smartphone on which they had downloaded the application. As such, StopCovid was subject to the provisions of the constitution and international conventions concerning the right to respect for private life and to those of the data protection regulations, notably

[66] Decree no. 2020-650 of 29 May 2020 concerning "StopCovid" data processing.

[67] Olivier Faye and others, '« L'application StopCovid retracera l'historique des relations sociales » : les pistes du gouvernement pour le traçage numérique des malades' *Le Monde.fr* (8 April 2020) <https://www.lemonde.fr/planete/article/2020/04/08/stopcovid-l-application-sur-laquelle-travaille-le-gouvernement-pour-contrer-l-epidemie_6035927_3244.html> accessed 19 July 2021.

[68] Alexandra Bensamoun and Nathalie Martial-Braz, 'StopCovid : sortir des postures ! Point de vue sur l'avis de la CNIL' [2020] Dalloz IP/IT 280.

[69] CNIL, 'Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid »'.

the GDPR. Moreover the system processes health data, a category of personal data afforded particular protection.[70]

Before its publication, the decree of 29 May 2020 for the development of StopCovid was reviewed by CNIL again.[71] CNIL considered that the processing was in the public interest, necessary and proportional. The recognition of proportionality was based on several guarantees contained in the draft decree and consistent with those previously announced by the Minister of Health and the Secretary of State for Digital Affairs, such as the absence of geolocalisation of individuals and the voluntary basis of participation. Proportionality was also apparent from the attempt to minimise the data recorded: *"the application will only collect data that are suitable, relevant and limited to those necessary to achieve the purposes for which they are being processed*".[72] In particular, the decree ruled out the collection of data "*enabling the identification of the mobile telephone, its owner or its user*",[73] which are not relevant to the objective. The time-limited duration of the system also manifested its proportionality: the decree stipulated that implementation of the application would end six months after the end of the state of health emergency. Here again the duration was redefined by subsequent amendments to the decree that postponed the end date to 31 January 2023,[74] i.e. much later than six months after the end of the state of health emergency.

Pseudonymisation of data is an additional guarantee provided by StopCovid, one also consistent with the principle of proportionality. StopCovid uses the ROBERT ('robust and privacy-preserving proximity tracing') protocol that organises the circulation of data as pseudonymised data with a limited lifetime: every telephone (*not* every person) is associated with a random pseudonym, i.e. a

[70] Art. 9 of the GDPR.

[71] CNIL, 'Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid »'.

[72] ibid.

[73] ibid.

[74] Decree no. 2022-1098 of 30 July 2022 modifying decree no. 2020-650 of 29 May 2020 concerning "TousAntiCovid" data processing.

code or a number independent of the real identity of the telephone's owner.[75] When Bluetooth is activated on the phone, the app collects and records the pseudonyms of other users of the app who also have Bluetooth enabled and are in close proximity. In this way, a 'close-proximity history' is generated on the phone and it stores each data point for fifteen days. If a user is diagnosed with Covid-19, they receive a single-use code from their doctor and a QR code is issued by SI-DEP. They can then decide whether to self-declare as infected in the application. If they do, it is the pseudonyms of high-risk contacts that are transferred to the central server; i.e. their own pseudonym is not transferred. The central server stores the pseudonyms then notifies exposed individuals, via the application on their smartphone, that they were in close proximity to another user who tested positive for Covid-19 in the last two weeks; no additional information is sent about the infected user's identity. The server also sends high-risk contacts useful information and encourages them to contact a doctor. Notably, the protocol used by StopCovid is unequivocally *not* a list of people with Covid-19, not even a pseudonymised version of one. CNIL considered that this protocol "*protects the private life of people concerned*".[76]

As per the GDPR, the purposes of data processing must be explicitly stated. The decree of 29 May 2020 enumerates four: to inform, to raise awareness and to guide contacts at high risk of infection; and to improve the performance of the system. As such, the decree excludes any intention to create a list of infected people, to track people's movements, to contact high-risk contacts directly, to monitor compliance with lockdown measures or to track people's social interactions.

The government also opted for *'public task'* as the lawful basis of StopCovid and *'reasons of public interest in the area of public health'* as the derogation condition for processing health data.[77] As with SI-DEP and Contact Covid, it circumvented the need to obtain the consent of the people concerned.

[75] Inria and Fraunhofer AISEC, 'ROBERT : Un Protocole de Suivi Des Contacts Respectueux de La Vie Privée' (18 April 2020) <https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-summary-FR.pdf> accessed 16 January 2022.

[76] CNIL (n 94).

[77] Decree no. 2020-650 of 29 May 2020 concerning "StopCovid" data processing.

However, as announced, StopCovid is a voluntary application: every individual is free to choose whether to download it on to their smartphone. Here, the voluntary basis should not be considered the lawful basis of the processing but rather a way of improving "*acceptability"* and *"trust in the tool*",[78] as was the absence of negative consequences (notably discrimination) for those who did not use it.

The decree also granted people concerned the right to be informed about the main characteristics of processing and about their rights. In line with CNIL's recommendations and in contrast to the initial draft text, it does not derogate the right to object nor the right to erasure, which are both fully respected.[79] In contrast, it rules out the possibility of exercising the rights of access, of rectification and to restrict processing, which CNIL recognises as legitimate, along with the exclusion of the right to data portability. With regard to the right of access, CNIL considered consultation of the data would be "*of very limited value for the person concerned and unrestricted consultation by any person obtaining the smartphone on which the application was installed would weaken the security of the system*".[80]

Despite all these precautions, the StopCovid application is not devoid of risks to data confidentiality. Pseudonymised data are by definition not anonymised data as per the GDPR, insofar as it is still possible to attribute them to a specific person by triangulating with other data. Hence there is a risk that people can be identified.

2. *The Possibility of Infected People being Identified by Users*

[78] Bensamoun and Martial-Braz (n 91).

[79] Cécile Crichton, 'StopCovid : parution du décret portant création de l'application' (*Dalloz Actualité*, 4 June 2020) <https://www.dalloz-actualite.fr/flash/stopcovid-parution-du-decret-portant-creation-de-l-application#.YPfqIugzbIU> accessed 16 January 2022.

[80] CNIL (n 94).

One of the notable characteristics of the StopCovid application is that it alerts *"in a systematic manner and without discernment all people who were in close proximity to the infected person*",[81] provided that it has been activated and that the close-proximity criteria defined by the order are met. This is a characteristic that distinguishes it from other situations, such as when infected people alert people they know informally and contact tracing by Contact Covid, in which infected people may choose not to reveal the identity of their contacts.

This characteristic introduces new risks, including the possibility that users are able to determine, if they want to and without resorting to sophisticated hacking techniques, whether people they have been physically close to are infected. The developers of the ROBERT protocol had foreseen this possibility, insisting on the need to ensure that contact tracing applications should not be able to be transformed into *"spy tools by their users, notably to know whether people […] have been diagnosed.*"[82]

In practice, anyone (the 'snoop'), whether or not a health professional, can find out whether another person (the 'target') has become infected if the target is using StopCovid. All the snoop needs to do is to install the application on their smartphone, but only activate Bluetooth when close to the target, all the while making sure that no-one else is in close proximity to their smartphone. After the two people part ways, the snoop deactivates Bluetooth; if they receive an exposure alert they can be certain that the target has self-declared as infected. In short, this simple technique allows the exposure alert to be attributed to infection of a specific person. Moreover, it is difficult to neutralise this possibility because, in the words of François Letellier, IT engineer and former member of the National Institute for Research in Digital Science and Technology (*Institut national de recherche en sciences et technologies du numérique,* INRIA), "*the system cannot impose a minimum number of contacts before sending out an alert because (…) it should in theory work for individuals who have very few daily*

[81] Xavier Bonnetain and others, 'Le traçage anonyme, dangereux oxymore' <https://hal.inria.fr/hal-02997228> accessed 16 January 2022.

[82] Inria and Fraunhofer AISEC (n 96).

contacts".[83] Furthermore, if such a minimum number were implemented, this protection could easily be overcome by creating fake users or enlisting the help of other complicit users who promise to not declare any infection.[84] It should be added that the possibility of identifying an infected person is not always attributable to malicious intent: an individual who receives an exposure alert and who has only been in contact with one other application user in the preceding two weeks can easily deduce that the other application user has self-declared as infected. Ultimately, as the researcher puts it: *"the only way of guaranteeing your confidentiality in the event that you become infected is… to not declare the infection*".[85]

In addition, the combination of the StopCovid application and an application that records the user's movements could be used to determine the location of infected patients with a certain degree of precision. Once an exposure alert were received by several users, one would proceed by cross-referencing the recorded movements.[86] Although the infection status of a given person would not be revealed immediately, it could be revealed with further investigational work.

Finally, it is possible to deduce that a person has not declared an infection by the fact that the application is activated. This follows on from the fact that the protocol deactivates the application when the user self-declares as infected, which was implemented to limit the possibility of determining whether a specific person was infected. However, there remains the possibility that a user is infected but has not been tested or has not self-declared the infection in StopCovid. Once again, the best way one can claim to not be infected is to not declare one's infection in StopCovid.

---

[83] François Letellier, 'Attaques de Désanonymisation Par Inférences Contre Les Utilisateurs d'une Application de Traçage de Contacts En Situation Épidémique (COVID-19, StopCovid)' <https://www.researchgate.net/publication/341056981_Attaques_de_desanonymisation_par_inferences_contre_les_utilisateurs_d%27une_application_de_tracage_de_contacts_en_situation_epidemique_COVID-19_StopCovid> accessed 16 January 2022.

[84] ibid.

[85] ibid.

[86] Bonnetain and others (n 112).

3. *Risks Inherent to Centralised Systems*

Given that the protocol contains a central server controlled by the data controller, in this case the Minister of Health, StopCovid was categorised as a centralised – as opposed to a decentralised – system.[87] The French government thereby limited the power accorded to users. In decentralised systems, adopted in most countries,[88] the pseudonyms of people who test positive (rather than those of their contacts) are communicated to the application of *all* other users. The application of the other users automatically checks whether received pseudonyms match any of those contained in the close-proximity history of the smartphone. Thus, the pseudonyms of all people who self-declared positive are present in the smartphones of all application users. Given that every smartphone contains a list of all self-declared positives, some have characterised decentralised systems as *"decentralised centralisation*".[89] Despite the fact that the list is in pseudonymised form, there is still a risk that users will be able to reidentify the people behind the pseudonyms. The cryptologist Serge Vaudenay considers that "*decentralisation creates more threats to privacy than it removes*", even though it is often presented, almost dogmatically, as inherently better.[90]

As stated above, centralised systems also present risks because data pseudonymisation does not fully prevent people from being reidentified: by combining pseudonymised data with other data collected

[87] '« Contact tracing » : Bruno Sportisse, PDG d'Inria, donne quelques éléments pour mieux comprendre les enjeux' (18 April 2020) <https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux> accessed 16 January 2022.

[88] European Parliament. Directorate General for Parliamentary Research Services., *Lifting Coronavirus Restrictions: The Role of Therapeutics, Testing, and Contact Tracing Apps: In Depth Analysis.* (Publications Office 2020) <https://data.europa.eu/doi/10.2861/7568> accessed 16 January 2022.

[89] '« Contact tracing » : Bruno Sportisse, PDG d'Inria, donne quelques éléments pour mieux comprendre les enjeux' (n 100).

[90] Serge Vaudenay, 'Analysis of DP3T - Between Scylla and Charybdis' <https://www.semanticscholar.org/paper/Analysis-of-DP3T-Between-Scylla-and-Charybdis-Vaudenay/52e5b3c53054bdbdc39644e2b1a791d418c0762e> accessed 16 January 2022.

by the device, or external to it (such as data collected via Bluetooth), it can become possible to determine the identity of a person – even if the short life of pseudonyms is designed to significantly complicate the task.[91] Consequently, systems like this require a high degree of trust in the health authority overseeing them. For example, if the authority were able to reidentify the individuals behind the pseudonyms transferred by the infected person's device to the central server, it would not have access to the identity of the infected person (as only the pseudonyms of high-risk contacts are transferred), but it would have a list of people at risk of developing the disease.[92] Then it could reach the conclusion that individuals who had previously been exposed to Covid-19 and who are in the list did not quarantine as they were supposed to.[93] This eventuality was even more regrettable in view of the fact that in the first version of the application, the entire close-proximity history was sent to the central server when a user self-declared Covid-19. Filtering of high-risk contacts occurred centrally, even though this operation was supposed to be performed on the user's phone and was contrary to the provisions of the decree of 29 May 2020. The government corrected this anomaly after receiving formal notice from CNIL.[94]

[91] Bonnetain and others (n 112).

[92] ibid.

[93] ibid.

[94] Decision no. MED-2020-015 of 15 July 2020 constituting formal notice to the Ministry of Solidarity and Health.

CONCLUSION

Faced with a pandemic of unprecedented scale in the 21st century, the French government implemented two distinct contact tracing systems to slow the spread of Covid-19: MCT carried out by healthcare system stakeholders and DCT based on a smartphone application downloaded by citizens. These systems, deployed soon after the end of the first lockdown, reflected the desire to deploy solutions that were less restrictive to individual freedoms and more compatible with a normal level of activity. Their stated purposed excluded any intention of tracking the movements of individuals, monitoring their social interactions or checking compliance with prescribed measures.

The legislator applied a derogation to the principle of confidentiality so that positive results of tests done by laboratories and the identity of contacts collected by doctors could be declared to health authorities. However, instead of incorporating the derogation into the existing list of notifiable diseases, it was accompanied by the development of two new information systems. Although several guarantees were provided, for example that no sanctions would be applied to infected people who refused to participate in contact tracing, the legislator's decision raised serious issues in relation to respect for private life, in terms of the extent of the data transferred and the number of people with access to the data, both going far beyond what was permitted with the notifiable diseases system. The limited duration of the information systems was an important guarantee but subsequent legislation completely broke the 'mechanical' link with the end of the state of health emergency; now their end date will have far outlived the state of health emergency.

In DCT, individuals who have chosen to download and install the StopCovid application to their smartphones are alerted when they have recently come into contact with an infected individual. The alert does not require the intervention of any healthcare system stakeholders because the application uses Bluetooth technology to build close-proximity contact history. DCT complements MCT in that it alerts individuals not known to the infected person but who have come into close proximity with them. Nevertheless, DCT also poses its own risks. In itself and regardless of the protocol used, the decision to use a DCT application exposes the risk that non-healthcare professionals are able to identify the infection of a third person. Furthermore, even though decentralised systems are not devoid of risks, a

centralised system could be exploited by the central controlling authority to collect information on application users.

Although MCT and DCT are intended to be used in different situations (MCT attempts to identify and contact the contacts declared by infected people, while DCT alerts contacts that infected people do not know personally hence cannot identify), in reality there are many situations in which MCT and DCT are overlapping rather than complementary. It is entirely possible that StopCovid alerts a close friend of the infected person if both individuals had their applications active when they were in close proximity, and that the friend has already received or will receive an alert after being identified by MCT. The advantage of overlapping is that the infection risk alert may arrive sooner, so a test can be performed sooner and contacts enter quarantine sooner; the downside is that there are more risks to privacy from two methods than one alone. To prevent the accumulation of risks, a user would need to make sure the application was not active when in the presence of people they know or to not divulge the identities of at-risk contacts during interviews with MCT stakeholders.

In view of the fact that CNIL declared both these information systems compatible with the GDPR, should we conclude that the GDPR does not provide sufficient protection or that CNIL was too lax? Undoubtedly, it is the case that CNIL diligently sought to ensure the proportionality of measures at a time when the pandemic was raging. The respect for private life should not automatically rule out the search for a compromise solution aimed at protecting public health. Moreover, as an alternative to lockdowns, contact tracing could help to preserve individual freedoms, such as freedom of movement, and to protect the economy. It could even, in the long run, make it more likely that all restrictions are lifted. Despite the ambitious goals, scientific evidence demonstrating the effectiveness of contact tracing in the fight against Covid-19 has to date been limited.[95] Some countries decided against

[95] Kelly Jean Thomas Craig and others, 'Effectiveness of Contact Tracing for Viral Disease Mitigation and Suppression: Evidence-Based Review' (2021) 7 JMIR public health and surveillance e32468; Thiemo Fetzer and Thomas Graeber, 'Measuring the Scientific Effectiveness of Contact Tracing: Evidence from a Natural Experiment' (2021) 118 Proceedings of the National Academy of Sciences of the United States of America e2100814118.

developing a DCT application,[96] yet did not have higher mortality rates than France.[97] Finally, although CNIL gave the green light to the contact tracing systems at their launch, it also later denounced the fact that the government had not provided justification for continuing to use these methods.

[96] 'Applications mobiles de traçage des contacts dans les États membres de l'UE' (*Commission européenne - European Commission*) <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_fr> accessed 23 January 2022.

[97] Ritchie and others (n 2).